IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	EWALD	:	Group Art Unit:	3625
Serial No.	10/672,133	:	Examiner:	Smith, J.
Filed:	09/26/2003	:	Confirmation No.	6111
For:	SYSTEM AND METHOD FOR PURCHASING LINKED WITH BROADCAST MEDIA	:	Attorney Docket No. 49663.21740	

DECLARATION OF WALTER E. THAIN, JR., PURSUANT TO 37 C.F.R. §1.132

I, Walter E. Thain, Jr., hereby declare and aver as follows:

1. I make this declaration of behalf of the Applicant. I am paid an hourly rate for my review of the materials of this application and present testimony, but otherwise have no affiliation with or financial interest in the Applicant, or financial or other interest in the eventual outcome of the present application.

2. I am an Associate Professor of Electrical Engineering Technology (ECET) at Southern Polytechnic State University (SPSU) in Marietta, Georgia. I have been an Assistant or Associate Professor at SPSU since August, 1997. I have a Bachelors Degree, Masters Degree, and Doctorate Degree in Electrical Engineering from the Georgia Institute of Technology.

3. I teach courses at graduate and undergraduate levels in the areas of wired and wireless communications systems, and computer networks and the Internet. While employed by private industry either full-time or as a part-time consultant, I have participated in electronic communications system development projects.

4. I am familiar with the patent application 10/672,133, by Applicant Ewald, and the patent application 09/867,687 by *Kesling, et. al.* I am also familiar with the Patent Examiner's decision regarding the claims of Ewald and position on the interpretation of *Kesling*, as well as the results of Appeal Number 2006-1365. I have been asked to render my evaluation as to whether the use and effect of the button 1220 in the portable radio 20 described in *Kesling* enables the purchase of goods or services immediately when pressed.

ANATOMY OF A PURCHASE TRANSACTION

5. Before addressing the use and effect of the button 1220 in *Kesling*, it is important to examine the steps and operations that take place during a purchase transaction. The example used here is that of a typical retail store purchase; however, the same steps are required in an electronic purchase transaction. Below, I describe eight key steps that occur when a buyer makes a purchase at a retail store.

i) The buyer indicates to the seller or the seller's employee (a cashier), that he wishes to start a purchase transaction. In a retail store, this is done by arriving at the cashier's station with the items to be purchased.

ii) The buyer then identifies to the cashier the items to be purchased by placing them on the cashier's counter.

iii) The seller (cashier) indicates a recognition or registration of the items to be purchased. This is done by actions such as picking them up to read the price, or scanning the item using a bar-code scanner. The latter enables the simultaneous retrieval of price from the store's inventory data base as well as the decrementing of the store's inventory totals.

iv) The communication of the total cost of the purchase by the cashier to the buyer.

v) The presentation of the means of purchase to the cashier by the buyer. In a retail store, this is usually the presentation of cash, a check, a credit card, or a debit card. The latter three essentially constitute a granting of permission by the buyer to the seller to access the buyer's checking or credit account for the purpose of debiting it by the amount of the sale. Also, the latter three means of purchase usually require the buyer to present a form of identification or authorization. Identification and authorization often includes, photo ID cards, verification of signature, or the buyer's entering of a personal identification number (PIN) to the terminal that records the buyer's credit- or debit-card number. The PIN is a unique secret code associated with the credit or debit card.

vi) An acknowledgement by the seller (cashier) of the receipt of the buyer's means of payment. For a cash or check transaction, this is done when the cashier receives the cash or check in hand and enters the amount paid into the cash register followed by pressing a key on the cash register to initiate payment processing. For a credit- or debit-card transaction, the cashier waits until the buyer enters the credit- or debit-card number and PIN (if required) into the terminal and then presses a key on the cash register to initiate payment processing.

vii) Processing of the payment. In the case of a cash or check payment, the processing is trivial and the cashier places the money or check in the cash register till, returning any change due and a paper receipt to the buyer. In the case of the credit- or debit-card payment, a third party entity is contacted when the cashier presses the button to initiate payment processing. The third party entity receives the buyer's identity and account information from the seller along with the amount of the sale, and then informs the seller as to whether or not enough funds are available in the checking account (in the case of a debit card) or available within the credit card limit to cover the purchase. The seller or third party entity will debit the buyer's account at the time of purchase or at some later time. The conveying of the buyer's identity and credit- or debit-card numbers to the third party is done over a secure electronic communication link, usually involving encryption (scrambling) of the number so as to make it impossible to determine the card number even if the transmission is intercepted. Once the third party verifies available funds to cover the purchase, the cashier gives a paper receipt to the buyer.

viii) Release of the purchased items. Once the payment is complete and the cashier gives the buyer a receipt, the buyer is granted permission to take possession of the purchase items and remove them from the store.

6. Of these eight steps, clearly the most complex actions involve the processing of the buyer's debit- or credit-card number. These same actions also require attention to the buyer's privacy rights by all parties involved in the process. Systems designed to process such means of purchase are typically complex and sophisticated. I

have attached several references that illustrate types of debit- and credit-card payment processing systems and considerations in their design at a level of refinement at about the time of the *Kesling* application date.

7. Attached hereto as Exhibit A is S. Weinstein, Emerging Telecommunications Needs of the Card Industry, *IEEE Communications Magazine*, vol. 22, no. 7, July 1984. Weinstein gives several examples of debit- and credit-card payment system topologies employed circa 1983. The Internet was in its infancy at this time and communication between the point-of-sale terminal (or cash register in the above example) was typically made over dial-up lines or lines leased from the public telephone network. In 1983, encryption of the transaction data was beginning to be implemented for privacy and security purposes.

8. Attached hereto as Exhibit B is L. J. Camp and M. Sirbu, Critical Issues in Internet Commerce, IEEE Communications Magazine, vol. 35, no. 5, May, 1997. Camp and Sirbu discuss key issues in Internet commerce circa 1997, one of which is the increasing use of open, packet-switched networks to carry transaction traffic. Issues such as reliability, privacy, anonymity, and security are discussed.

9. Attached hereto as Exhibit C is U. S. Patent 5,850,442, issued December 15, 1998, to S. Muftic, titled "Secure World Wide Electronic Commerce Over An Open Network." Muftic describes a secure electronic commerce system. Security is provided in part by encryption of transmitted purchase transaction information using the public-key technique. One must note the complexity of the transaction system and processes included in Muftic's invention.

ON THE USE AND EFFECT OF BUTTON 1220 IN KESLING'S RADIO 20

10. It is my opinion that in order to enable the purchase of a good or service by the action of pressing button 1220 in radio 20, this one action must immediately cause to take place all eight of the steps and actions described in the example purchase transaction above. Further, since the button 1220 is located in a mobile radio 20, such a purchase transaction must take place over a combination wireless and wired electronic communication system. The last link between the communication system and radio 20 must be wireless as described in *Kesling*.

11. The system described in *Kesling* makes use of wired and wireless communication links depending on what actions are taking place and where the operator (listener or buyer) is located. [See e.g., Figs. 2 and 3 and Paragraphs 26 through 39 of Kesling] Those skilled in the art understand that such links are mere conveyers of information. The only processing of the original information to be communicated that occurs is that needed to facilitate the communication act along the communication path. This involves formatting the original information, converting it to a signal appropriate for transmitting on the chosen physical transmission medium, transmitting it across the physical medium, routing the information along the appropriate path, receiving the signal at the destination, and reformatting it into its original form at the destination. The actions of formatting information and converting it to appropriate signals for transmission usually include placing the information in digital data frames, or packets, then modulating a transmitter carrier signal with that information. At intermediate nodes along the path, the signal may be received, demodulated, re-modulated, and retransmitted as required by a particular communication link in the path. Finally, at the destination, the demodulation process includes the recovery of the original transmitted information. Apparatus along the communication link do not act upon the information being conveyed in the data frames other than using a limited amount associated with the physical communication process itself, such as routing addresses.

12. An electronic communication system itself, including the one described in *Kesling*, is not capable of the high-level processing needed to facilitate complex actions such as processing the payment information exchanged in a purchase transaction. To do that, computers running appropriate software applications along with data bases of stored records must be attached to the communications system at the end points.

13. In the system described by *Kesling*, one skilled in the art can see how radio 20 may be utilized to receive broadcast content containing program identifier information as described in paragraph 39 thereof. Further, one can also see how pressing button 1220 at an appropriate time will result in storing program identifier information in the storage media 1140. Also, it is apparent that the high-power wireless transmitter 700 and low-power wireless transmitter 600 included in radio 20 may be

used to form a communication link to convey information from radio 20 back to an entity or server elsewhere in *Kesling*'s system. It is further apparent that pressing button 1220 can cause information to be sent over one or both of the radio 20 transmitters.

14. Considering the eight steps of a typical electronic purchase transaction, one sees that when a listener (buyer) presses button 1220 in radio 20, the system as described by *Kesling* can readily perform steps 1, 2, 3 and 4 immediately. However, the description of the system makes no mention that when button 1220 is pressed that there is communication of payment information (such as debit- and credit-card numbers) from the buyer to the seller. There is no mention that payment information (such as credit- and debit-card numbers) is stored in radio 20. Also, there is no mention that when button 1220 is pressed that there is any further processing of payment information and debiting of the buyer's account. Thus, neither steps 5, 6, 7, nor 8 take place when button 1220 is pressed. The process and actions involved in conveying payment information and completing a purchase transaction at the press of button 1220 would be complex and require a sophisticated method to properly and securely handle such information. Such a process and methodology are not described in *Kesling*.

15. Therefore, in my opinion, pressing button 1220 does not enable a complete purchase transaction in the system described by *Kesling*, as is suggested by the Patent Office.

I hereby declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge.

Dated this 19th day of June, 2006, signed at Marietta, Georgia, U.S.A.

Walter E. Thain Jr.

Walter E. Thain, Jr.

Exhibit A

Emerging Telecommunications Needs of the Card Industry

Stephen B. Weinstein

Development and proliferation of the communications infrastructure for authorization and broader transactional capabilities

THE CARD INDUSTRY offers a wide range of payment system products and services, including credit and charge cards, automatic-teller machine networks, interchange networks, debit card systems, authorization and processing services, and point-of-sale equipment. The trend in the industry is to extend automation in the forms of both on-line and off-line transactional systems to a vastly increased number of points of sale and to personal terminals in business and home locations. To this end, the industry is increasingly interested in interchange among proprietary and industry networks, traffic concentration and other facilities sharing arrangements, conversion of voice traffic to data traffic, use of cable television and other local-loop bypass options, integration of public packet-switched networks with private networks, and enhanced transactional security and authentication.

Introduction

"Plastic money," in the form of credit cards, has existed as a widely used payment system for only 25 years, but hundreds of millions of cards are in use around the world. They give cardholders the privilege of paying later for goods purchased now, and the revolving credit loans automatically granted when payments are delayed beyond the first monthly billing are an important part of consumer credit. Credit card issuers, mainly banks and large retailers, earn income from three sources: a percentage "discount" in the remuneration of merchants, interest from revolving credit, and recently, from membership fees.

Other types of plastic money also exist, although not in quite such large quantities. The American Express and Diners' Club cards are examples of charge cards, similar to credit cards except for the absence of revolving credit. Issuers position charge cards as "travel and entertainment" payment media and ask higher merchant discount and card membership fees to make up for the absence of interest income. A third type of payment card, the debit card, automatically draws funds from an existing bank account, usually within one day. The cards used in automatic teller machines to obtain cash are debit cards and are perhaps the precursors of true electronic money at points of sale. The important difference between debit cards and the others, as far as operational systems are concerned, is that the instructions to transfer funds in debit systems are made by electronic communications instead of paper.

All three types of payment cards do share one very important telecommunications need: credit authorization. Credit authorization is a reference to a credit file, with or without the intercession of a human operator, to establish that the card is not stolen and that the cardholder can be expected to pay for the purchase. Credit authorization has been automated to the point that a purchase made in a distant country, at least one made through an automatic terminal, can be authorized in seconds from the card issuer's central data base. A vast array of proprietary, shared, and interconnected data networks has been created to service this need. The further development and proliferation of this data communications infrastructure, its accommodation of limited voice traffic, its containment of costs, its responsiveness to external pressures, and its evolution into broader transactional capabilities, particularly full electronic funds transfer, define the emerging telecommunications needs of the card industry.

Reprinted from the *IEEE Global Telecommunications Conference Record* (GLOBECOM '83), Nov. 28-Dec. 1, 1983, San Diego, CA.

0163-6804/84/0700-0026 $01.00 © 1983 IEEE

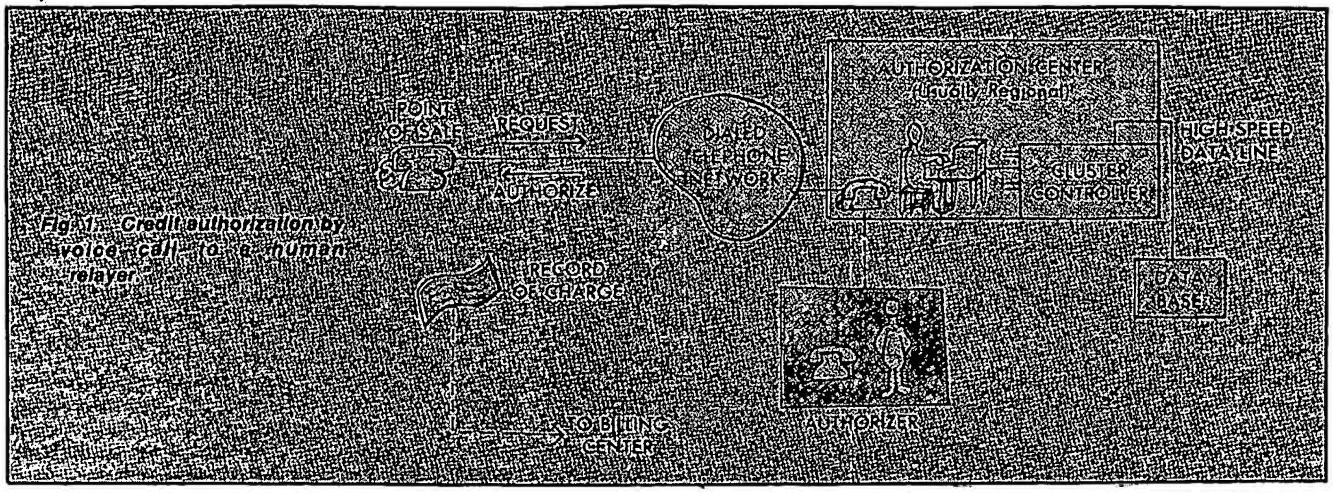


Fig. 1. Credit authorization by voice call to a human relayer.

On-Line Credit Authorization

The agreement between a merchant and a card issuer obligates the issuer to take responsibility for fraudulent or "bad credit" purchases only if the merchant calls into the issuer for credit authorizations. Actually, a merchant may be asked to call in only for authorization of purchases above a certain "floor" amount, especially if he is not equipped with an automatic data terminal and must use the telephone. Below the floor, the merchant is asked to use the printed "hot list." Because of the inadequacies of the hot list, card issuers want to automate lower-traffic points of sale with very-low-cost data communications and data terminals, thereby permitting on-line inquiries for virtually all card purchases. This drive for both universality and low cost determines the most fundamental and immediate telecommunications needs of the card industry. Some of the steps underway to meet these needs are described later.

As suggested above, credit authorization is carried out through a variety of telecommunications accessing methods. Figure 1 illustrates voice call-in to a "relayer" at an authorization center; the relayer is seated before a terminal which is in direct data communication with a central data base. Files are accessible to the relayer with a delay of no more than a few seconds. This service can be expensive because of its labor intensity and the cost of the telephone call from point of sale to authorization center.

An important additional operation is the "voice referral" made in about 5% of authorization calls to a human authorizer, an individual empowered to make credit decisions when the machine decision (from the data base) is ambiguous or the cardholder contests a rejection. The authorizer is ordinarily different from the relayer. Note also that funds transfer is handled separately, through use of paper records. Large retailers, such as airlines, may submit magnetic tapes of transaction records.

A second accessing method is via private-line data terminals on polled multipoint circuits connected directly to the authorization data base (Fig. 2). These terminals read the magnetic stripe on the back of a card and send the terminal's identification automatically, so that the sales clerk need only enter the purchase amount. This makes possible a very fast transaction, but is cost effective only at larger-volume locations. Card issuers have been taking steps toward regional concentration (Fig. 3) to reduce communications costs. Future communications strategies may emphasize access through public data networks and alternative local distribution facilities, as described later.

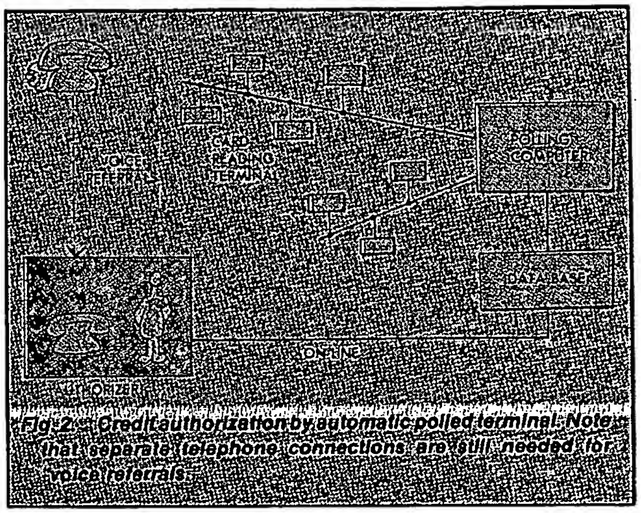


Fig. 2. Credit authorization by automatic polled terminal. Note that separate telephone connections are still needed for voice referrals.

A third accessing method is via automatic *dialup* terminals which, like voice calls, use the switched telephone network

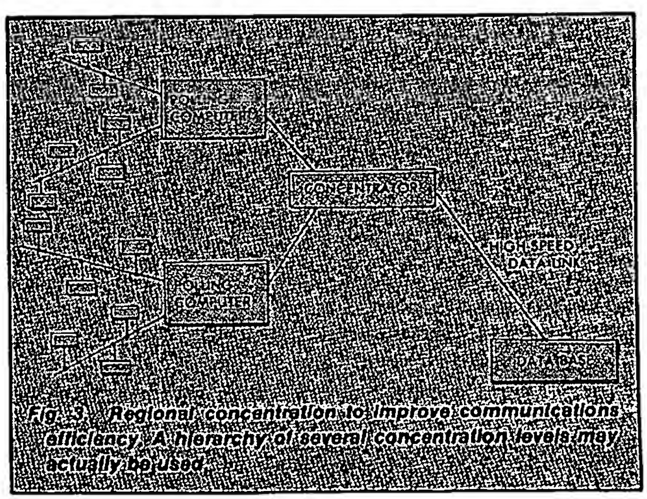


Fig. 3. Regional concentration to improve communications efficiency. A hierarchy of several concentration levels may actually be used.

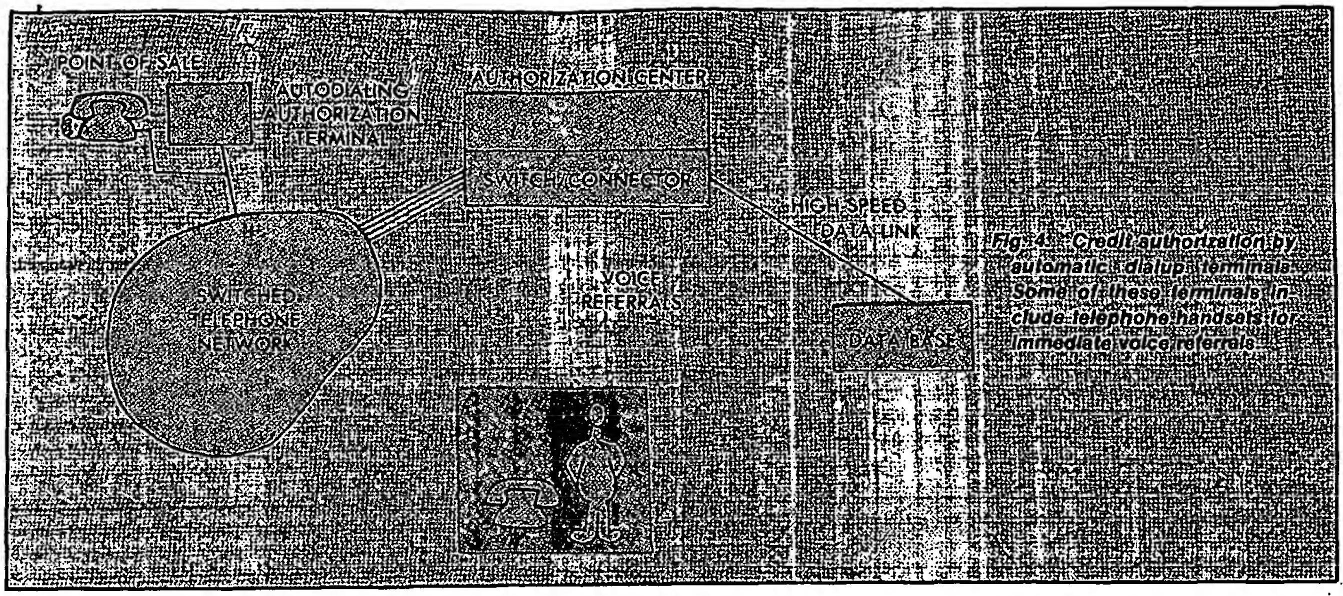


Fig. 4. Credit authorization by automatic dialup terminals. Some of these terminals include telephone handsets for immediate voice referrals.

(Fig. 4). This accessing method is attractive for points of sale without sufficient traffic to support a private line terminal, especially with the recent development of moderate-cost ($400) terminals complete with autodialers, modems, and magnetic stripe readers. If a telephone is available on the same line, voice referrals can usually be switched through the authorization center without a need for separate dialing.

The largest push in point-of-sale automation is in deploying these low-cost dialup terminals. A number of ways to reduce the high costs of dialed lines, and even the moderate cost of dialup terminals, are being tested or considered, with emphasis on regional concentration of various kinds. One technique (Fig. 5) is the use of automatic voice response units (ARU's), which are accessed by local phone calls from very-low-cost terminals, including pushbutton telephones, and concentrate data traffic for transmission to the distant data base. Canned voice prompts are provided to the calling sales clerks. Another technique (Fig. 6), increasingly used in Europe where national PTT's encourage the use of public data networks, is tandem connection through the dialed network and the public packet-switched network, with voice referrals automatically dialed by the point-of-sale terminal in response to instructions from special facilities monitoring the data traffic. The shared facilities of the packet-switched network are appropriate for the short, bursty traffic characteristic of credit authorization, but the need to provide occasional voice referral communications might be better met in a future integration of voice with data traffic.

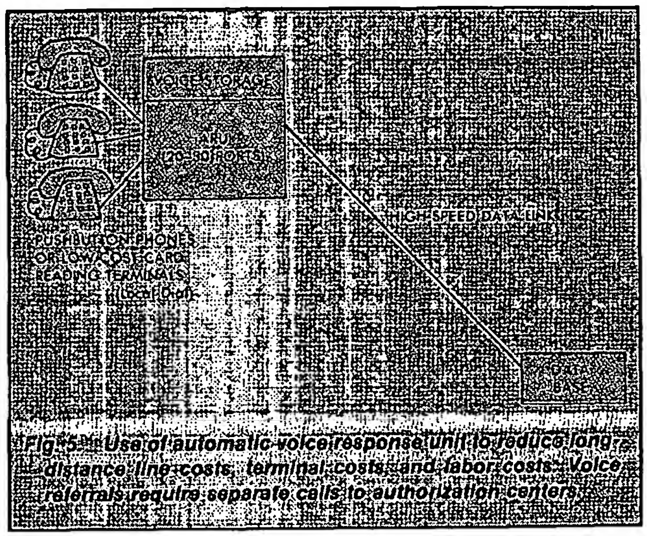


Fig. 5. Use of automatic voice response unit to reduce long-distance line costs, terminal costs, and labor costs. Voice referrals require separate calls to authorization centers.

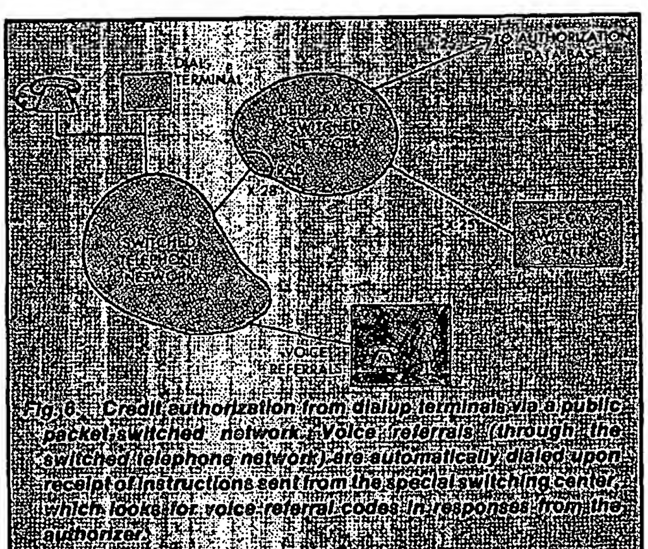


Fig. 6. Credit authorization from dialup terminals via a public packet-switched network. Voice referrals (through the switched telephone network) are automatically dialed upon receipt of instructions sent from the special switching center, which looks for voice-referral codes in responses from the authorizer.

Interchange and Shared Facilities

A fourth accessing method is via interchange (Fig. 7) with other institutions, including large retailers supporting their own point-of-sale systems and "third parties" providing interchange services. The rationale for interchange is, of course, to broaden the communications reach and terminal population for a particular card without that card issuer having to invest in additional facilities. Developing an interchange relationship requires some software development for the conversion of message formats and communications protocols, but it is more a business than a technical question. The

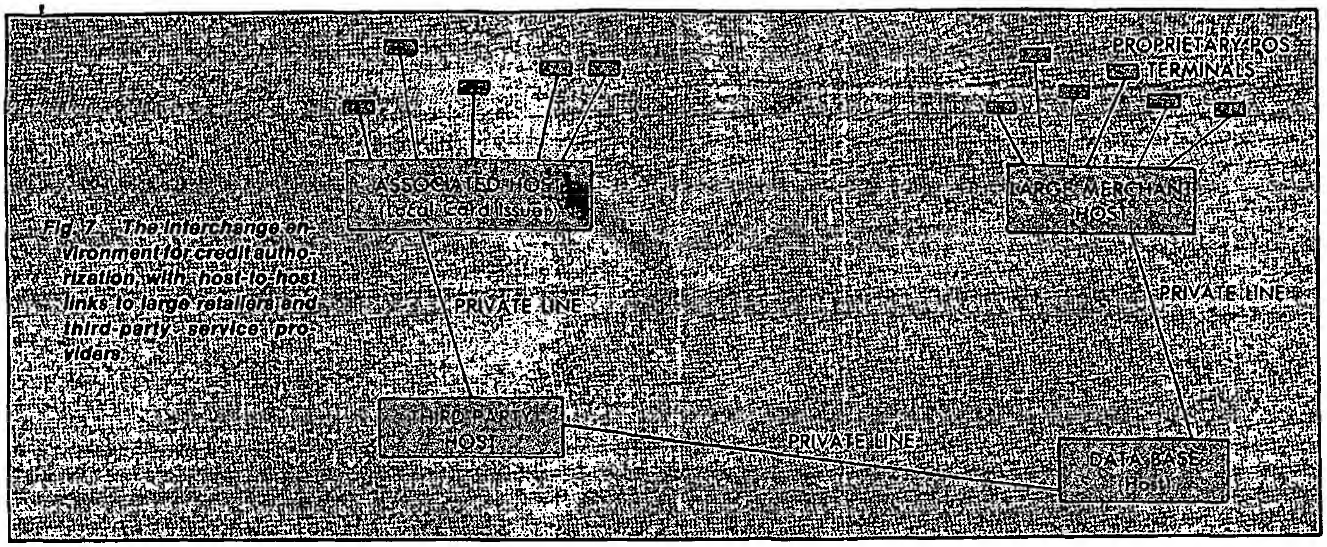


Fig. 7. The interchange environment for credit authorization, with host-to-host links to large retailers and third-party service providers.

communications needs are for dedicated computer-to-computer links, typically operated at 2.4 kb/s to 9.6 kb/s, and for appropriate backup facilities, dialed or private.

One interesting development seen in both proprietary and interchange environments, but particularly the latter, is truncation of communications through the use of distributed data files. An authorization data base will usually contain a "negative file" of bad cards, equivalent to the printed "hot list," which is clearly much smaller than the full "positive files" on all cardholders which constitute the bulk of the data base. This negative file can be distributed to regional processors (Fig. 8), so that calls for authorization on purchases with "bad" cards can be answered from the regional processor (with a rejection message) instead of from the distant full data base. In the interchange environment, this means that one card issuer may be housing and using data bases on cardholders of other issuers, illustrating the delicate balance between competition and cooperation which appears to be characteristic of communications-intensive businesses, and is, perhaps, creating new needs for privacy safeguards.

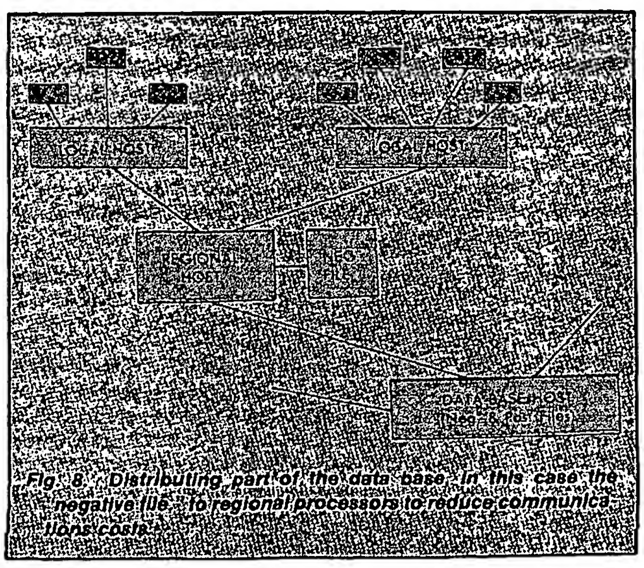


Fig. 8. Distributing part of the data base, in this case the negative file, to regional processors to reduce communications costs.

Optimization of credit authorization and other transactional networks with respect to the division between communications and distributed data basing and processing is one of the central problems of transactional networking, and one of the most interesting technically. It depends critically on technical and regulatory developments in the communications industry and on developments in memory and data-base technology. If communications costs increase and data storage and processing costs continue to decrease, data storage and processing functions may be replicated in local host computers or even in terminals themselves. A cheap, rewritable memory of several megabytes for use in transactional terminals can be considered a "need" of the card industry in the sense of opening up broader possibilities for decentralization of data access and processing functions.

One of the most striking recent developments in transactional interchange is the advent of the nationwide automatic teller machine (ATM) interchange network. Several competing networks are in fact being developed. This is a true, if not quite complete, electronic funds transfer (EFT) application at the personal level, with individuals using their "cash cards" to obtain cash at ATM's of banks other than their home banks.

As Fig. 9 illustrates, the ATM interchange network conveys identification information and an authorization request from the user to the host computer of his home bank. If this host computer is convinced of the identity of the user, conveyed through a personal identification number (PIN), an authorization for the transaction is returned to the host computer supporting the ATM. The reconciliation between the two banks is handled in a separate bulk transaction.

Network security becomes an important issue in this application. If the PIN is not encrypted for its transit through the network, or if the authorization message is not protected, the system becomes susceptible to fraud by both passive and active interceptors. "Good practice" now suggests link-by-link DES encryption for the PIN (as indicated in Fig. 9), but not all participating institutions are convinced of the need for security.

However, link-by-link encryption, with its stored keys and reencryption points, is weaker than end-to-end encryption with a unique "session key" for each transactional session. A pressing need of future personal EFT networks, including

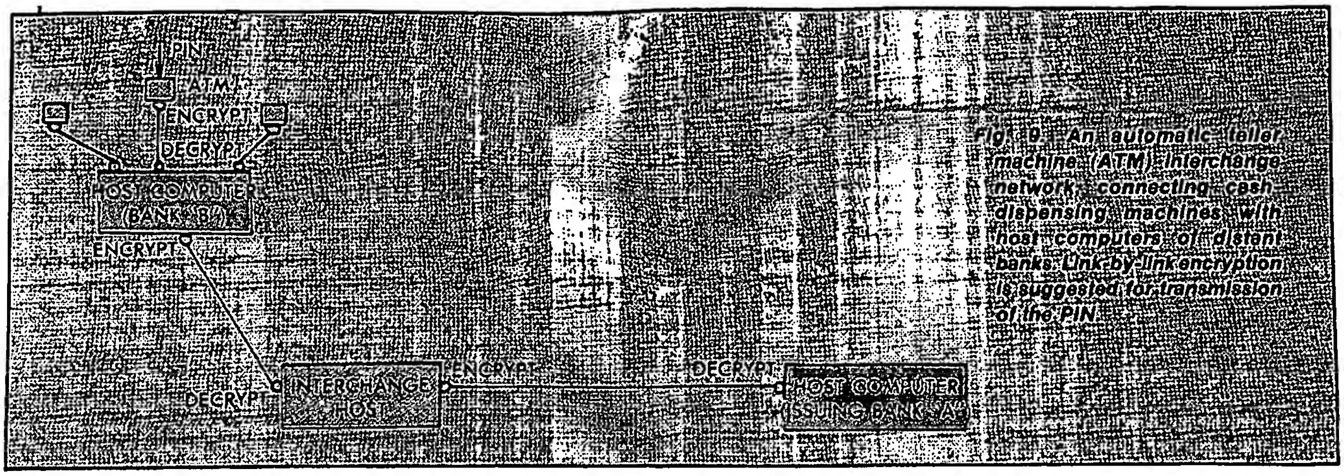


Fig. 9. An automatic teller machine (ATM) interchange network, connecting cash-dispensing machines with host computers of distant banks. Link-by-link encryption is suggested for transmission of the PIN.

"home banking" networks, is effective, simple, and cheap security and authentication technology. In fact, the whole phenomenon of transactional interchange networks invites new attacks on the integrity and privacy of personal and institutional data files which must be met with new technical safeguards.

New Media and the On-Line—Off-Line Choice

The efforts at data concentration described earlier (automatic voice response, regional concentrators, stored data networks) still leave the requirements for local communications. The card industry needs to hold down communications costs and improve performance in the local as well as the long-distance arena, but it has not made very much progress so far. Digital subscriber loops, as in the integrated services digital network (ISDN) or some of its forerunners, have the potential to offer faster exchanges at lower cost and satisfy some of the anticipated needs. Digital access will be particularly welcome if it does indeed integrate voice with data communications, carrying voice referrals through the same digital facilities with instantaneous increases (as requested) in assigned capacity.

Cable systems may also provide a local-loop bypass option, although interactive cable services are developing much more slowly than anticipated. The relatively low-capacity polling schemes used in some interactive cable systems may be able, in some locations, to support a population of transactional terminals. Unfortunately, CATV is usually not supplied to businesses, and transactional services alone may not justify the installation costs. And, even when cable is installed, it may be best to use its inherent efficiency as a *broadcast* medium to update remotely distributed credit files rather than to carry interactive traffic.

Other communications media have also been suggested, including low-rate two-way satellite communications between ATM's and host computers using spread-spectrum transmission techniques [1]. Microwave digital termination services may also be useful local distribution media. There is, in any event, a need to develop better local communications facilities for transactional communications.

A somewhat different view of transactional communications is taken by advocates of off-line rather than on-line commu-

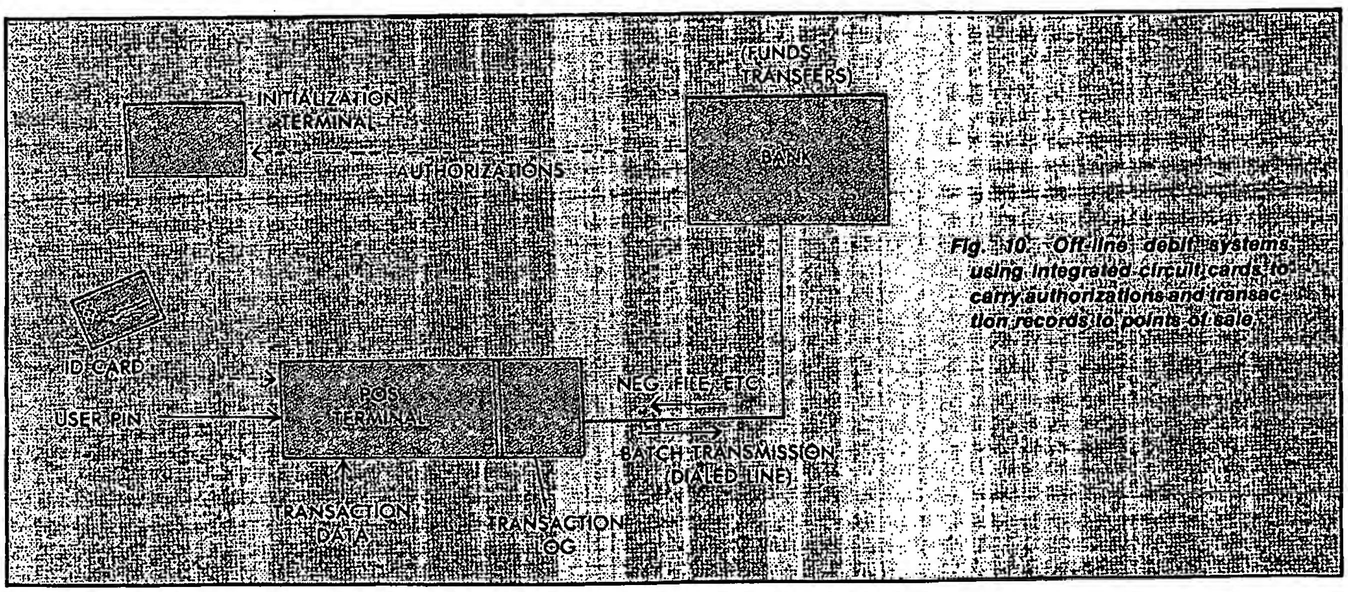


Fig. 10. Off-line debit systems using integrated-circuit cards to carry authorizations and transaction records to points of sale.

nications systems, particularly off-line systems using integrated circuit ("smart" or "chip") cards. In a debit system based on these cards (Fig. 10), credit authorization is granted on the strength of the authorization and transaction records in the customer's card and there is no call to a distant data base. Transaction records are also retained by the (off-line) point-of-sale terminal, which periodically transfers them in a batch transmission, through a dialed connection, to a clearing institution. A greater penetration of low-volume points of sale may be obtained with such an off-line system than with a conventional on-line system.

The Essential Telecommunications Needs of the Card Industry

The foregoing review of what the card industry does with telecommunications, and what it would like to do, has suggested a number of needs which enhanced telecommunications might help meet:

1) Lower cost per transaction.
2) Automation of smaller points of sale.
3) Facilities sharing and interchange to increase reach and restrain costs.
4) Minimization of voice traffic, and integration with data traffic.
5) Effective use of public data facilities.
6) Security and authentication techniques appropriate for EFT and for data-base privacy and integrity despite easier access.
7) More choice among communications alternatives, especially for local communications.
8) Serious consideration of distributed vs. central data management, and of (partly) off-line vs. on-line communications.

Acknowledgment

The author is indebted to a number of individuals in the credit card industry for their knowledge and advice.

Reference

[1] Private communication from Equatorial Communications Co., Inc.

Stephen B. Weinstein, born in New York City in 1938, received degrees in Electrical Engineering from M.I.T. (S.B. 1960), the University of Michigan (M.S. 1962), and the University of California Laboratories in Eindhoven, the Netherlands, he joined Bell Laboratories in Holmdel, NJ, where his work was largely in voiceband data communications.

In 1979, Dr. Weinstein left Bell Laboratories for a subsidiary of the American Express Company, Payment Systems, Inc., transferring in 1980 to the Office of Corporate Development and Planning of the parent company, where he advises management on technical issues.

Dr. Weinstein, an IEEE Fellow, is a member of the Board of Governors of the IEEE Communications Society and is the new editor-in-chief of *IEEE Communications Magazine*. He recently completed a three-year term as chairman of the editorial board of the IEEE Press. ■

Exhibit B

ABSTRACT

In this article the authors identify reliability, privacy, and security as critical issues in electronic commerce. In other work, designers of information systems have identified other issues as critical, such as the ability to provide offline verification. It is widely agreed that an electronic currency system must provide divisibility, scalability in number of users, conservation of money or tamper resistance, exchangeability or interoperability, and availability [1–6]. However, by returning to the fundamental definition of money and the essential nature of electronic information systems, the authors argue that privacy, reliability, and security are also critical issues. It is argued that these issues are particularly important in Internet commerce. The authors conclude by noting how some proposed Internet commerce systems provide, or fail to provide, security, reliability, and privacy.

Critical Issues in Internet Commerce

L. Jean Camp, Sandia National Laboratories

Marvin Sirbu, Carnegie Mellon University

Internet commerce is sending electronic payments over a public network to obtain electronic goods or commitments to deliver physical goods. Internet commerce will bring together consumers and merchants in transactions that cross jurisdictional boundaries on a scale that was previously as inconceivable as it was technically infeasible. In transactions that cross national boundaries, many questions which are now answered through force of law, such as consumer liability for a lost credit card number, may now be addressed through technical fiat. In this article we determine the critical policy issues which are being addressed at the design level by beginning with the basic properties of money. We will focus on the dominant issues in the design of electronic commerce systems: privacy and fraud.

Crucial questions in Internet transactions are: What can customers, merchants, and banks lose on the Internet? Who must they trust? And who takes the risks?

Answers to these questions vary across the multitude of proposed protocols for electronic commerce on the Internet. However, an examination of a broad range of these protocols makes clear that in electronic commerce, customers can lose both their money and their privacy. To protect privacy and money, Internet transactions must be secure, reliable, and anonymous.

Reliability and security are interdependent. The lack of reliability of an electronic commerce system can be exploited by attackers to commit theft. Reliability in electronic commerce may require security to provide authentication, integrity, and irrefutability. Reliability is not security. Reliable protocols on servers that are not secure will provide reliable services to attackers as well as to authorized users.

Privacy, anonymity, and security are distinct but interdependent properties. Privacy means that the subject of information can control the information. Privacy requires security, since security is control over information. However, security is not sufficient for privacy, since the owner and the subject of the information may have very different interests in and uses for the data. In fact, security may preclude privacy by ensuring that the subjects of information have neither control nor knowledge of the uses of that information. Anonymity means that information has no subject — that is, identity is not linked to the information. Thus, anonymity ensures privacy.

Obviously, security is necessary for the protection of both user funds and user privacy. However, security alone can protect neither.

Unlike surveillance threats, with anonymous currency illegal acts can be simplified. Risks of anonymous currency include transmitting threats and receiving related ransom anonymously, anonymous blackmail, tax evasion, and trivial money laundering.

We do not attempt to address every possible risk inherent in electronic commerce. It is already apparent that the advent of electronic funds transfer can magnify the weaknesses of cash control systems [7, 8] or entail unnecessarily detailed information gathering that threatens individual privacy laws [9–12].

WHY INTERNET COMMERCE?

Why the Internet? Why will commerce thrive on the Internet rather than in easier-to-manage intranets? Who is out there?

What is the Internet? And who is out there? The Internet began as the ARPANET, a United States government project for connecting scientific research sites. As late as 1986, when ARPANET became NSFNET and expanded its mission, the Internet community was dominated by researchers and scientists. It was not until 1990 that the first commercial e-mail provider, MCI Mail, was connected to NSFNET. But in the '90s, commercial information providers came onto the Internet along with commercial e-mail providers. Early adopters of Internet technology for information marketing include Dow Jones and Dialog [13]. Thus began Internet commerce. Since 1990 the growth of the Internet has been exponential. The growth of hosts on seven continents from the Internet Domain Survey [14] is shown in Table 1. It is these growth curves that so excite the providers of content and commerce services.

In 1989 Tim Berners-Lee developed a protocol to enhance data sharing for collaborative physics, the hypertext transport protocol (http). This protocol is the underlying technology for the World Wide Web. The Web allows consumers to search

0163-6804/97/$10.00 © 1997 IEEE

for information on the Internet with a straightforward graphical interface. Easy access to information has been a significant driver of Web growth. With http, the Internet became fully capable of supporting user-friendly distributed commerce, just as previous protocols had enabled functionality from simple communication to file transmission. The Web remains a critical element in emerging electronic markets.

Certainly the obvious answer to the question, "Why Internet commerce?" is "That's where the customers are." The other answer is that Internet commerce offers the potential to greatly reduce transactional overhead. Many successful business ventures are now on the Internet. Table 2 shows examples of businesses on the Internet and corresponding paper information markets [15].

Region	Hosts, 1/94	Hosts 1/95	Hosts, 1/96	Hosts, 1/97
North America	1,685,715	3,372,551	7,088,754	11,216,035
Europe, West	550,933	1,039,192	2,699,559	4,352,152
Europe, East	19,867	46,125	168,142	784,225
Middle East	6946	13,776	44,484	58,930
Africa	10,951	27,130	84,715	104,838
Asia	81,355	151,773	672,495	106,664
Pacific	113,482	192,390	475,505	647,948

■ **Table 1.** *Regional growth on the Internet.*

Market structure	Electronic example	Paper example
Publisher pays	Web catalogs	Mail order catalogs
Advertiser pays	Lycos, Yahoo	Free weekly papers
Club pays	ClariNet, site license software	Corporate library
Customer subscription	Web magazines, dlists	Professional magazines
Customers pay per item	FirstVirtual	Storefront sales
Customers pay for time	AOL, CompuServe	Rental items
Mixed ads and customer payment	Prodigy, Netscape business sites	Newspaper

■ **Table 2.** *Structure of information markets (dlists: distribution lists).*

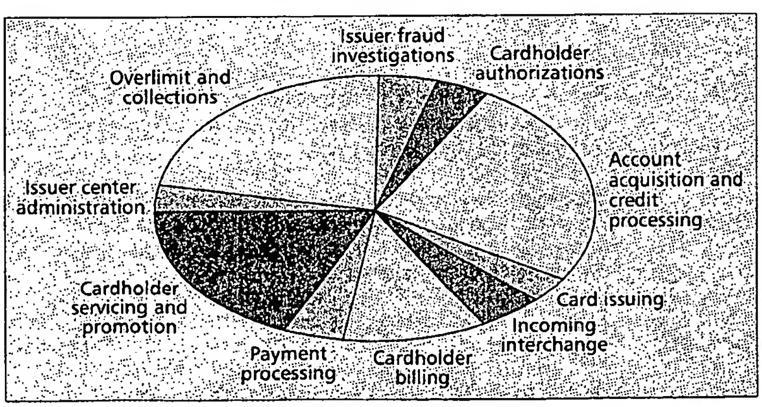
The Internet supports a range of business functions, not simply payment. Every transaction has multiple phases: product discovery, price negotiation, final selection, payment, delivery, and dispute resolution. The Internet can support many types and all stages of Internet commerce [16].

Product discovery is enabled on the Internet through advertising and electronic word of mouth. Product information is dispersed through Web pages, distribution lists, and Usenet groups. The Web enables individuals to locate specific information and search by product or company name. Corporate Web sites often exist solely for the purpose of distributing product information with a simple graphical interface. With distribution lists, or dlists, individuals who have a common interest form a closed group and transmit messages of interest to all members of this group. Announcements of new products are made by members of the dlist.

All the technologies consumers use to find out about services can also be used to locate suppliers. Web search engines, such as the hotbot and Lycos, also provide a simple way for consumers with Web access to locate products.

Price negotiation is supported by e-mail and electronic data interchange. Information goods can be delivered online. Customer support can be offered online through e-mail and via Web pages.

Every phase of a commercial transaction has associated costs. The ability of an Internet commerce protocol to reduce transaction costs depends on its ability to address these costs. For comparison, the distribution of costs in a credit card transaction is shown in Fig. 1 [16].



■ **Figure 1.** *Cost distribution in a credit card transaction.*

The value of Internet commerce partially depends on how the costs in the figure can be decreased through automation. The Internet allows administration of customer orders, payment or payment authorization transmission, and production of an invoice to be automated.

In addition to cost advantages through automation, the Internet allows services to be provided continuously, around the clock, around the globe, in multiple languages and currencies. Catalogs of merchandise can be found by interested shoppers at negligible marginal cost to the merchant. The catalogs seen by every consumer can be updated immediately as prices and inventory changes.

Internet commerce could affect the lives of millions. The standards which determine how money and information flow around the Internet are being determined now — and some of the fundamental decisions about the risks consumers will take are integrated as technical details in technical specifications. Examination of those specifications and enumeration of the risk are particularly timely while Internet commerce is yet infant and the standards are still in flux.

Money, Its Functions, and Electronic Commerce

Here we will answer two related questions: Why are reliable transactions important? And what are the properties of a reliable electronic commerce protocol? To answer these questions, we must first address a more basic

Unlike physical money, electronic money is merely bits, and thus can be trivially duplicated so that money can be stored in multiple locations.

issue: What is money? Defined by its three elemental functions, money is a store of value, a standard of value, and a medium of exchange [17]. Money as a medium of exchange requires reliability in transactions, and providing transactional reliability in electronic commerce is not trivial.

Money as a store of value requires durable storage. For money to be a store of value, it must not be easy to destroy or create. If money decays or is destroyed in storage, it obviously does not succeed in storing value. In contrast, hyperinflation illustrates the failure of money as a store of value when it can too easily be created. Under hyperinflation, entire nations are forced to abandon money and return to barter.

Durable storage is necessary for electronic commerce. Unlike physical money, electronic money is merely bits, and thus can be trivially duplicated so that money can be stored in multiple locations. Note that this duplication of money differs from the creation of money only when the duplicates cannot be spent; thus, ease of duplication is a double-edged sword. Furthermore, some electronic currency systems have money that expires in order to reduce the cost of a security violation. Thus, value of stored money, though not the bits themselves, could effectively disappear.

Money as a standard of value requires *interoperability*;[1] that is, to serve as a standard of value, any specific form of money must be either itself widely used (a standard) or readily convertible to a standard form. In the electronic environment, interoperability in terms of wide use means that a protocol can be implemented on many and diverse platforms. This type of interoperability is encouraged by open standards. Low requirements for participation in electronic commerce also encourage interoperability through wide use, by expanding the base of possible customers. Restrictions on participation have the reverse effect. For example, the requirement that electronic commerce customers have a credit card [18] prohibits the participation of anyone without a credit history and significant income.

Interoperability in terms of convertibility means different vendors' software can exchange data; in electronic commerce, converting money amounts to exchanging data. Interoperability is not an insurmountable issue, since even systems that are not secure [19] can provide interoperability.

Money as a medium of exchange requires special transactional properties. The transactional properties that enable money to serve as a medium of exchange amount to transactional reliability. Therein lies the answer to our initial question: why are reliable transactions important? Reliable transactions in electronic commerce are important because they are necessary to the proper functioning of electronic money as a medium of exchange.

Reliable protocols can provide certainty in the face of network failures, memory losses, and electronic adversaries. An unreliable electronic commerce system cannot distinguish a communications failure from an attack. If a failure can be used effectively for theft, then certainly such attacks will occur.

There remains, then, the second question: what are the properties of a reliable electronic commerce protocol? The study of distributed databases has defined the characteristics of reliable database transactions as atomicity, consistency, isolation, and durability. These are known as the *ACID* properties. Physical transfers of money illustrate the ACID properties of a reliable transaction. ACID properties are innate in exchanges of physical money.

ACID transactions are atomic, consistent, isolated, and durable. Distributed ACID transactions are robust and can prevail in the face of network outages, replay attacks, failures of local hardware, and errors of human users [20].

Transactions are *atomic* in the Newtonian sense; they cannot be split into discrete parts. An atomic transaction either fails completely or succeeds completely. Funds are conserved in an atomic transaction. For example, consider what happens when a customer transfers funds from a savings account to a checking account. Either the checking account is credited and the savings account is debited, or neither account balance changes. There is no case where money either disappears from both accounts or is credited to both accounts.

If a transaction is *consistent*, all relevant parties agree on critical facts of the exchange. If a customer makes a one-dollar purchase, then the merchant, the customer, and the bank (if it is involved) all agree that the customer has one less dollar and the merchant one more.

Transactions that do not interfere with each other are *isolated*. The result of a set of overlapping transactions must be equivalent to some sequence of those transactions executed in nonconcurrent serial order. If a customer makes two one-dollar transactions, the two payments should not be confused. The customer should not end up being charged twice for one item, nor should one single payment be counted twice to give the two-dollar total.

When any transaction can recover to its last consistent state, it is *durable*. For example, if the customer physically drops a dollar when making a purchase, that dollar does not disappear. When the customer retrieves the dollar, the last consistent state is restored. Similarly, money that was available to a computer before it crashed should not disappear when the machine reboots.

Atomicity, consistency, durability, and isolation in a transaction create the possibility for irrefutability in electronic commerce. Suppose a customer wants to make a purchase from the local software store. The customer must pay, or promise to pay. The merchant either gets payment or proof of intent to pay in a standard purchase order or check. The customer gets a receipt from the merchant indicating that she has paid and expects the merchandise to be delivered. When it is delivered, the customer signs a receipt for the merchant indicating delivery has occurred. Each action is linked with some verification of action, so both parties have some proof in case the other party attempts fraud.

Electronic commerce systems have widely varying scopes, some covering only payment, while some address everything from negotiation to delivery. Different electronic commerce systems offer different degrees of atomicity to address the problems of remote purchases: money atomicity, goods atomicity, and certified delivery [21].

Of course, electronic transactions may have no atomicity. No atomicity requires mutual trust among participants. The physical equivalent is sending cash or goods in the mail to a post office box. Customer or merchant fraud can be simple in systems with no atomicity.

Electronic transactions may have money atomicity. The physical equivalent is paying cash in person. In money-atomic systems there is no mechanism for certification of merchandise delivery. If used for remote purchase with accepted techniques for the delivery of physical goods, money atomicity is quite adequate. But fraud, through a customer's theft of

[1] *This does not imply interoperability in the software engineering sense*

goods or a merchant's refusal to deliver goods after payment, can be trivial when systems with only money atomicity are used for goods with online delivery, such as software. Among the systems here, both anonymous credit cards [4] and Secure Electronic Transactions have money atomicity [18].

Electronic transactions may have goods atomicity. Goods atomicity corresponds to using a certifiable payment mechanism with certified delivery in a physical transaction. Goods atomicity provides high reliability and reduces the opportunity for merchant fraud. Goods atomicity is the equivalent of collect on delivery. The merchant is not paid unless there is a delivery; the customer does not pay unless there is a delivery.

Under the standard Transmission Control Protocol (TCP), a payment may be duplicated when the communications protocol believes the packet containing the payment message was lost on the network. Moreover, a payment message may be destroyed by network failure.

Finally, electronic commerce systems may provide certified delivery. With certified delivery the customer certifies to the merchant his intent to order goods of a certain description, and the merchant warrants that what the customer received is what the merchant intended to deliver. While a decision as to whether what was delivered actually matches what was ordered is a semantic judgment, the ability to verify these items after the fact provides a powerful mechanism to ensure that the customer receives precisely what was agreed upon. NetBill offers certified delivery.

Atomicity depends on design, implementation, and business policy. Atomicity depends on funds-available policies because of rollback. Rollback is a technique where all steps are recorded and then reversed until the most recent consistent state is reached. For example, if a customer's attempt to transfer funds from checking to savings fails, funds withdrawn from the customer's checking account are placed back into the customer's checking account.

In electronic commerce, a payment message must travel over an open network, which is not secure, from the customer to the merchant. Without verifiable acknowledgment in the protocol, the customer will not know that the merchant received the payment message. Under the standard Transmission Control Protocol (TCP), a payment may be duplicated when the communications protocol believes the packet containing the payment message was lost on the network. Moreover, a payment message may be destroyed by network failure. If a payment message is lost, delayed, or destroyed, confusion rather than consistency may result.

Note that financial transactions as well as database transactions can also be classified as reliable using these properties. In some systems the financial transaction consists of one distributed database transaction, so in this case the application of these concepts is trivial. In other systems a single financial transaction requires multiple database transactions. In this case the failure of individual messages may require state changes in multiple database transactions for the financial transaction to remain atomic, since the scope of the financial transaction includes multiple database transactions. In short, transactional reliability is not a trivial matter in electronic commerce.

Rollback is complicated when financial transactions consist of multiple database transactions. For example, suppose a customer orders a free ticket as a frequent flyer award and includes a credit card number to pay for the courier charge. If the entire fare is mistakenly charged to the card, rollback is possible. However, it requires coordinating three databases: the airline frequent flyer database, the airline billing database, and the billing database of the credit card company. This is obviously more complex in computing and organizational overhead than simply redepositing unused funds at a single institution.

Superficially, electronic transactions are just exchanges of bits, and if the exchange can be reversed, the transaction can be made atomic. But for Internet commerce to expand, there must be some interoperability not only between forms of Internet commerce but also between Internet currency and traditional forms of money. Therefore, if the rollback period is too large the fraudulent party could abscond with unrecoverable cash, making the later acquisition of bits meaningless. This implies that a transaction which implements atomicity using rollback, and is theoretically atomic, may not be truly atomic. Using two-phase commit solves this problem by requiring that the record or funds are locked until global commit is issued. (At the point of global commit, all parties agree that the transaction has been completed.) This implies that for rollback to be useful, funds should remained locked until commit so that the money cannot be converted in the interim.

Providing customer anonymity is another critical issue. In physical exchanges of money, maintaining customer anonymity is trivial. The merchant present at the transaction may gather some information about the customer through direct observation, but no unique identifying information is recorded and stored as a result of the transaction itself, and no identifying information can be correlated with the purchase. In contrast, electronic commerce is fundamentally the manipulation of computerized records. Purchase information, including customer identity, is easily correlated across electronic transactions.

Issues of atomicity and anonymity are complicated by the definition of the scope of a transaction. When does a transaction begin? When does it end? What is the relevant scope of concern in a transaction? The information transmitted in a transaction varies if the transaction includes discovery, where the information available to the merchant depends on the Web browser used by the customer, or if the transaction includes only the purchase of the goods. As illustrated in the previous discussions of atomicity, the degree of atomicity depends on the scope of the transaction as well.

Currently published token currencies have not considered entire transactions, and therefore do not provide money atomicity. Token currencies illustrate the possible trade-off between atomicity and anonymity suggested in the discussion of rollback.

Digicash [22] is the canonical anonymous currency. Yet Digicash has no atomicity [23]. In the later version of Digicash, [24], Chaum attempted to provide money atomicity, through encoding identity into each token to be spent. Encoding identity allows double-senders to be identified, thereby resolving the conflict between anonymity and accountability in the case of double spending. The addition of integrity provides sufficient information for dispute resolution in issues of payment, but not enough information to resolve disputes over goods delivery.

MicroMint [25], which uses hashing rather than public key operations to affordably generate large quantities of electronic cash, offers no money atomicity in its simplest form. In order to provide money atomicity, MicroMint is extended so that customer identity is included in every coin. Thus, the extension of MicroMint to provide money atomicity depends on the requirement that every consumer identify herself to the merchant to verify her right to spend a coin.

Similarly, an analysis of protocols for Internet commerce

based on notational currency illustrates that reliability can be simplified by creating a single ledger. The creation of a single ledger means that there is a concentration of information, thus implying a threat to privacy. The Anonymous Credit Card protocol attempts to address this by accepting the increased complexity as the cost of privacy. However, the relationship between distribution of information and provision of privacy does not always hold true in that increased centralization does not always imply decreased privacy. NetBill, for example, has more centralized transaction processing than Secure Electronic Transactions but provides an equivalent level of customer privacy.

The designers of electronic commerce systems are implementing their values as well as their engineering creativity into the financial infrastructure.

CLOSING

In summary, the designers of electronic commerce systems are implementing their values as well as their engineering creativity into the financial infrastructure. In some cases the trade-offs made by the designers is explicit, as in MicroMint. However, in some cases the trade-offs result from adherence to previous models (as with SET) or are based on an implicit assumption that anonymity is worth the price of fraud (as with Digicash). In all cases, the policy choices and value decisions should be made in a open and democratic way rather than by quiet technical fiat.

Today the decision of whether to allow an electronic commerce offering is made in a regulatory cloud. Providers of electronic commerce are currently allowed to make spurious claims of anonymity, as in the case of Mondex [26]. Consumers and citizens are not given the information necessary to select electronic commerce systems that reflect their own preferences, with marginal costs, susceptibility to fraud, and desire for privacy all clearly defined.

Of course, some requirements for consumer identity are based on outdated regulatory models of records and are not under the control of system designers. Legal requirements for receipts, billing, contracts, and nonrepudiation do not reflect the potential for anonymous atomic systems or other technological capabilities. However, even with legal considerations, much remains in the hands of system designers.

We would argue that the Code of Fair Information Practice should apply to all transactions; in particular, consumers should know of records as they are being created and be able to opt out. Just as companies offering credit are required to explain the charges, designers and companies offering electronic commerce software should be required to explain what information about the user is made available.

Currently, electronic commerce system designers are choosing the risks consumers take between their wallets and their privacy. These decisions are inherently value-laden, and should be made with the recognition that issues of fraud and privacy cannot be addressed through post hoc regulatory solutions on the Global Information Infrastructure.

REFERENCES

[1] S. Brands, "Untraceable Off-Line Cash in Wallet with Observers," *Advances in Cryptology — CRYPTO '93*, Berlin: Springer-Verlag, 1993, pp. 302–18.

[2] L. J. Camp, "Privacy and Reliability in Internet Commerce," TR CS-CMU-96-198, Carnegie Mellon Univ., Pittsburgh, PA, 1996.

[3] Cross Industry Working Group, "Electronic cash, tokens and payments in the National Information Infrastructure," http://www.cnri.reston.va.us:3000/XIWT/documents/dig_cash_doc/ToC.html, Sept. 1995.

[4] S. Low, N. F. Maxemchuk, and S. Paul, "Anonymous credit cards," *Proc. First ACM Conference on Computer and Communications Security*, Nov., 1993.

[5] G. Medvinski and B. C. Neuman, "NetCash: A Design for Practical Electronic Currency on the Internet," *Proc. 1st ACM Conf. Comp. and Commun. Security*, Nov. 1993.

[6] T. Okamoto and K. Ohta, "Universal Electronic Cash," *Advances in Cryptology— CRYPTO '91*, Berlin: Springer-Verlag, 1991, pp. 324–36.

[7] M. J. Fischer, "Focus on Industry," *J. Accountancy*, June, 1988, pp. 130–34.

[8] P. F. Mayland, "EFT Network Risk Begs CEO Attention," *Bank Mgmt.*, vol. 10, no. 69, Oct. 1993, pp. 42–46.

[9] B. J. Compaine, *Issues in New Information Technology*, Norwood, NJ: Ablex, 1988.

[10] E. Fenner, "How Mortgage Lenders Van Peek into Your Files," *Money*, April 1993, pp. 44–48.

[11] C. Chaves, "The Death of Personal Privacy," *Computerworld*, Jan. 1992, pp. 25–27.

[12] W. Madsen, *Handbook of Personal Data Protection*, New York: Stockton Press, 1992.

[13] V. Cerf, "How the Internet Came to Be," *The On-line User's Encyclopedia*, ed. B. Aboba, Reading, MA: Addison-Wesley, 1993.

[14] Internet Domain Survey (IDS), Hosts Stats by County, http://www.nw.com/zone/WWW/isoc-pr-9501.txt, Nov. 1995.

[15] V. Goradia *et al.*, "NetBill: 1994 Prototype," Carnegie Mellon Univ., Pittsburgh, PA, 1994; available as INI tech. rep. INI TR 1994-11.

[16] M. Sirbu and J. D. Tygar, "NetBill: An Internet Commerce System Optimized for Network Delivered Services," *Proc. IEEE ComCon*, San Francisco, CA, Mar. 6, 1995.

[17] L. Rubin and R. Cooter, *The Payment System: Cases Materials and Issues*, St. Paul, MN: West, 1994.

[18] Mastercard, 1996, "Secure Electronic Transaction Technology," Draft., http://www.mastercard.com/SETT.

[19] First Virtual, "Information About First Virtual," http://www.fv.com/info, Oct. 8, 1995.

[20] J. Gray and A. Reuter, *Transaction Processing: Concepts and Techniques*, San Francisco, CA: Morgan Kaufmann, 1993.

[21] J. D. Tygar, "Atomicity & Electronic Commerce," *Proc. 1996 Symp on Principles of Dist. Comp.*, ACM Press, Philadelphia, PA, 1996.

[22] D. Chaum, "Security Without Identification: Transaction Systems to Make Big Brother Obsolete," *Commun. ACM*, vol. 28, Oct. 1985, pp. 1030–44.

[23] B. Yee, Using Secure Co-processors, Ph D. dissertation, Carnegie Mellon Univ., 1994; available as CMU tech. rep. CMU-CS-94-149.

[24] D. Chaum, "On-Line Cash Checks," *Proc. Advances in Cryptology — EUROCRYPT '89*, 1989, pp. 288–93.

[25] R. L. Rivest and A. Shamir, "PayWord and MicroMint: Two Simple Micropayment Schemes," Eurocrypt '96, 1996.

[26] G. Clark and M. Acey, "Mondex Blows Users' Anonymity," *Network Week*, vol. 1, no. 8, col. 1, Oct. 25, 1995.

BIOGRAPHIES

L. JEAN CAMP is a Senior Member of Technical Staff at Sandia National Laboratories in the Livermore facility. Her research interests are electronic privacy, particularly with respect to electronic commerce, and survivability. She completed her Ph.D. at Carnegie Mellon University (CMU) in engineering and public policy in 1996.

MARVIN SIRBU holds a joint appointment as professor in engineering and public policy, the Graduate School of Industrial Administration, and electrical and computer engineering at Carnegie Mellon University. His interests are in telecommunications and information technology, policy, and economics. In 1989 he founded the Information Networking Institute at CMU which is concerned with interdisciplinary research and education at the intersection of telecommunications, computing, business, and policy studies. Recent research activities have focused on electronic commerce, the economics of electronic publishing, compatibility standards in communications and computers, pricing of new telecommunications services, and new technologies for the local loop. He received his S.B., S.M., and Sc.D. degrees in electrical engineering from the Massachusetts Institute of Technology (MIT). Prior to coming to Carnegie Mellon in 1985, he taught at the Sloan School of Management at MIT, where he also directed its Research Program on Communications Policy.